FORCEnet engineering conference

November 15 -17, 2005: Town & Country Convention Center - San Diego, CA

Katrina Information Assurance (IA) Lessons Learned

Christopher Newborn

Security Architectures,

PEO C4I & Space PMW 160IA

17 November 2005

Approved for public release; distribution is unlimited (8 NOVEMBER 2005)

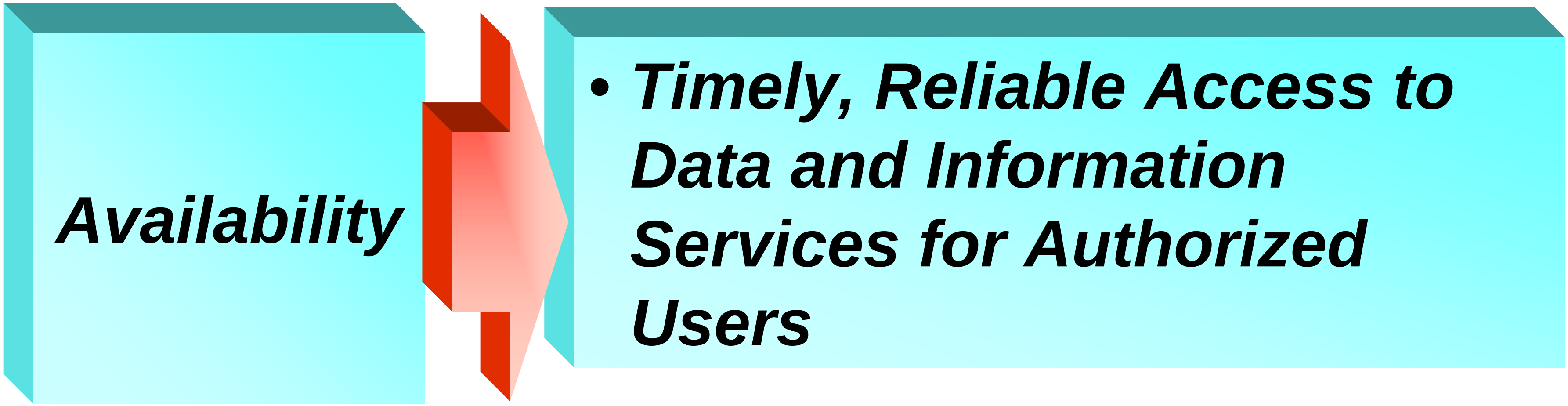
Sponsored by
SPAWARSYSCOM
FORCEnet Chief Engineer

Outline

- Defining IA Availability and Continuity of Operations (COOP)
- Katrina Background and Expectations
- Katrina Events/Situation Reports (SITREPs)
- Lessons Learned from NTCS Det New Orleans
- Summary
- Recommendations

What is IA Availability?

"Measures that Protect and Defend Information and Information Systems by Ensuring Their Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation. This Includes Providing for Restoration of Information Systems by Incorporating Protection, Detection, and Reaction Capabilities"



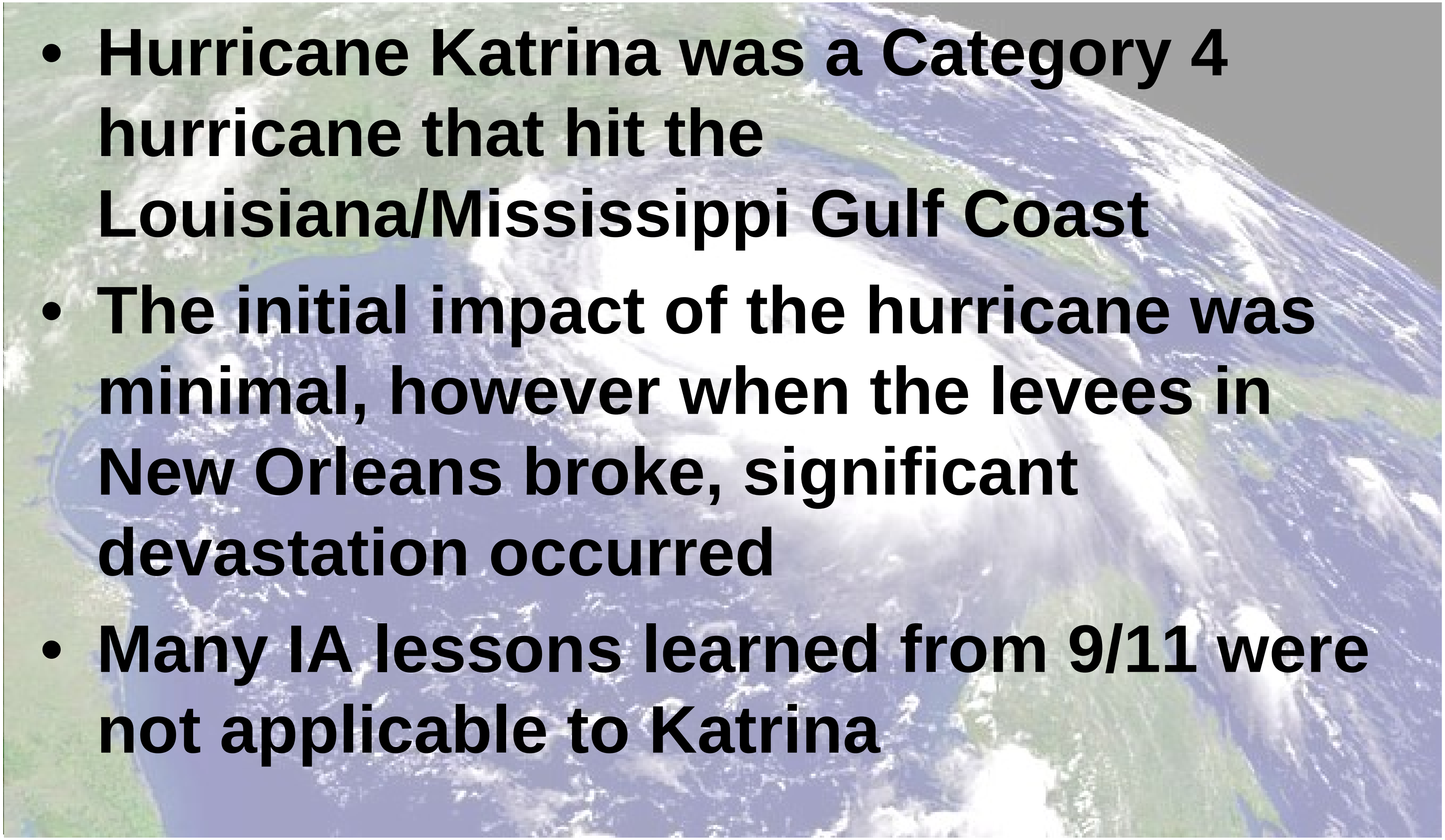
Availability

- ***Timely, Reliable Access to Data and Information Services for Authorized Users***

Continuity of Operations (COOP)

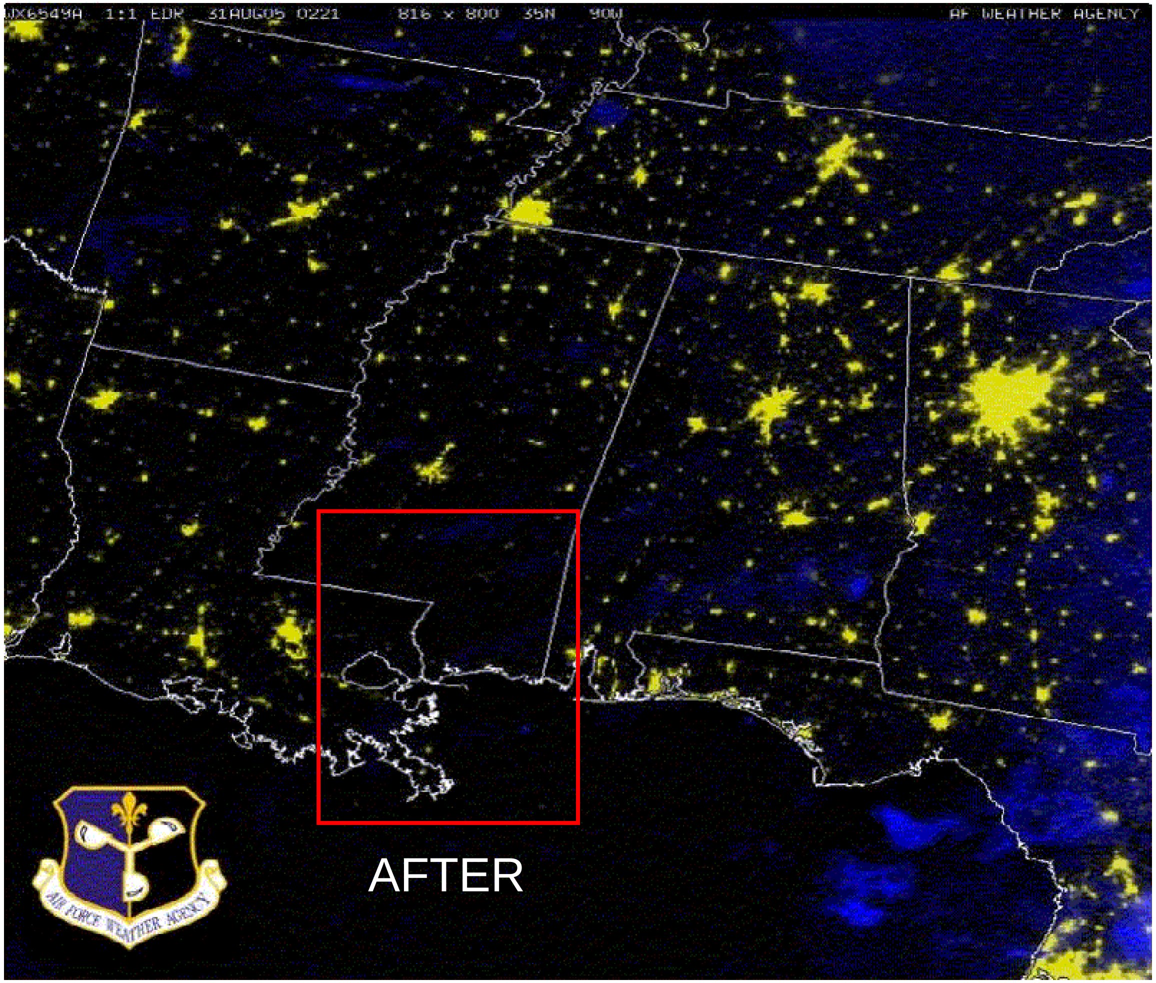
- **All military bases have some form of terrestrial services or commercial communications**
- **COOP plans include**
  - Specific procedures to implement before, during, and after an attack or natural disaster
  - Critical services required to support the mission
    - **Personnel**
    - **Equipment**
    - **Facilities/locations**
- **Key personnel needed to execute COOP**
  - Identify specific duties
  - Experienced/trained personnel
  - Prior disaster/recovery experience

Background



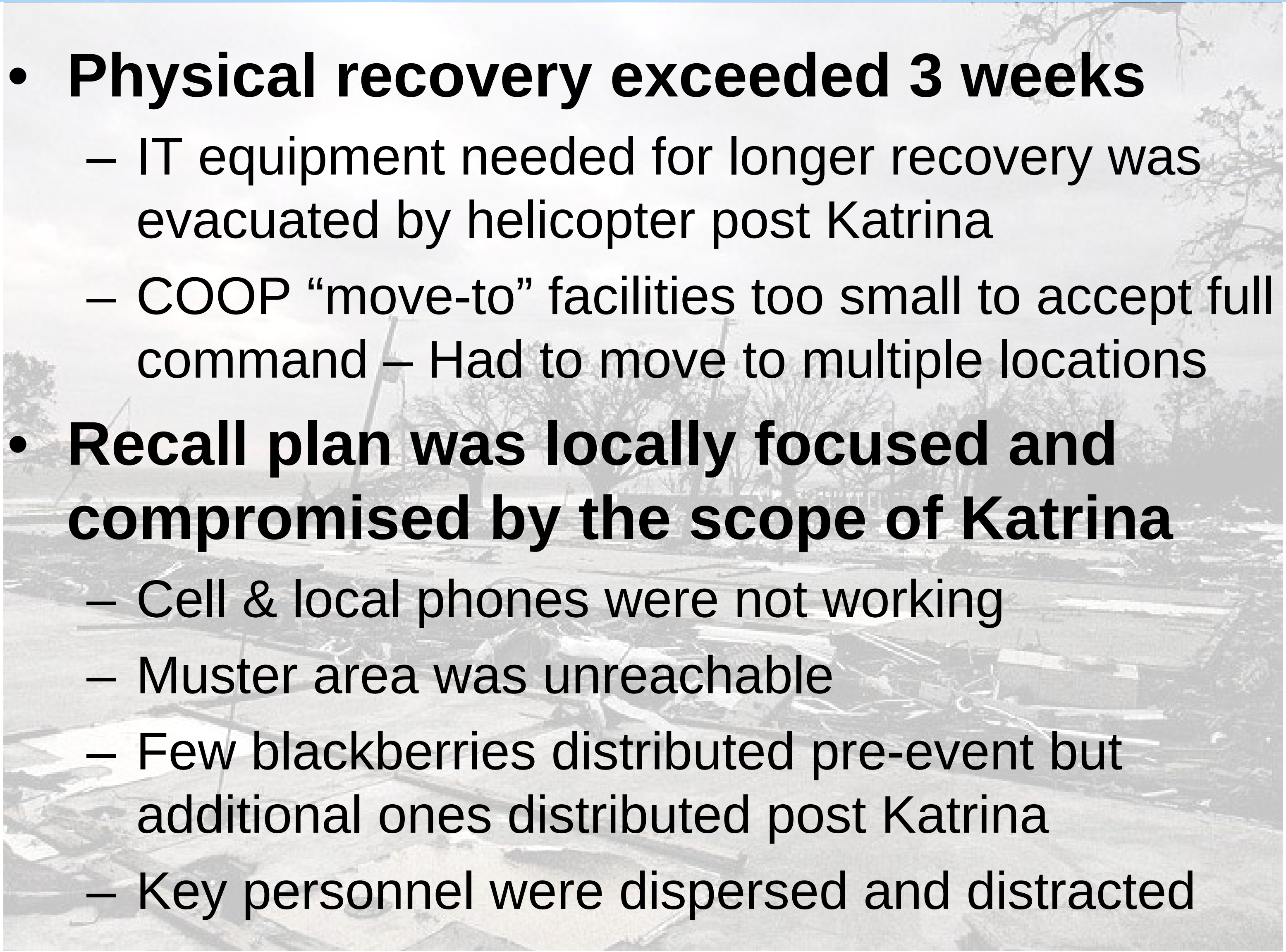
- Hurricane Katrina was a Category 4 hurricane that hit the Louisiana/Mississippi Gulf Coast
- The initial impact of the hurricane was minimal, however when the levees in New Orleans broke, significant devastation occurred
- Many IA lessons learned from 9/11 were not applicable to Katrina

Before/After Katrina



AFTER

Katrina Exceeded Planned Expectations



- **Physical recovery exceeded 3 weeks**
  - IT equipment needed for longer recovery was evacuated by helicopter post Katrina
  - COOP “move-to” facilities too small to accept full command – Had to move to multiple locations
- **Recall plan was locally focused and compromised by the scope of Katrina**
  - Cell & local phones were not working
  - Muster area was unreachable
  - Few blackberries distributed pre-event but additional ones distributed post Katrina
  - Key personnel were dispersed and distracted

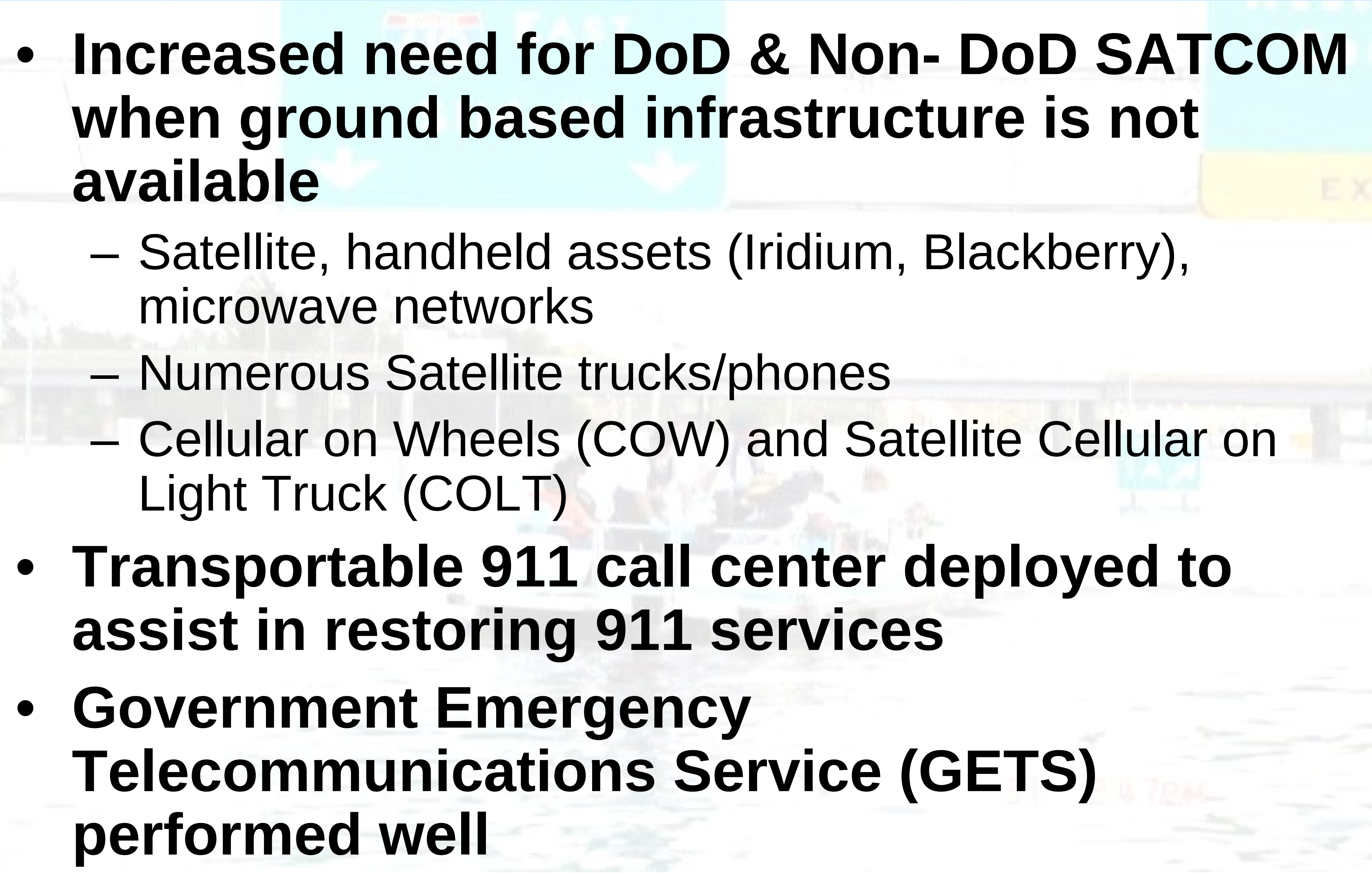
Katrina Events/SITREPs (GIG Status)

- **JTF-GNO status of the GIG was listed as "Green"**
  - Not Navy/NMCI or local base, camp, station perspective
  - Physical location & hierarchical position are important and impact perception
- **Isolated NIPR & SIPR outages in affected regions**

Availability

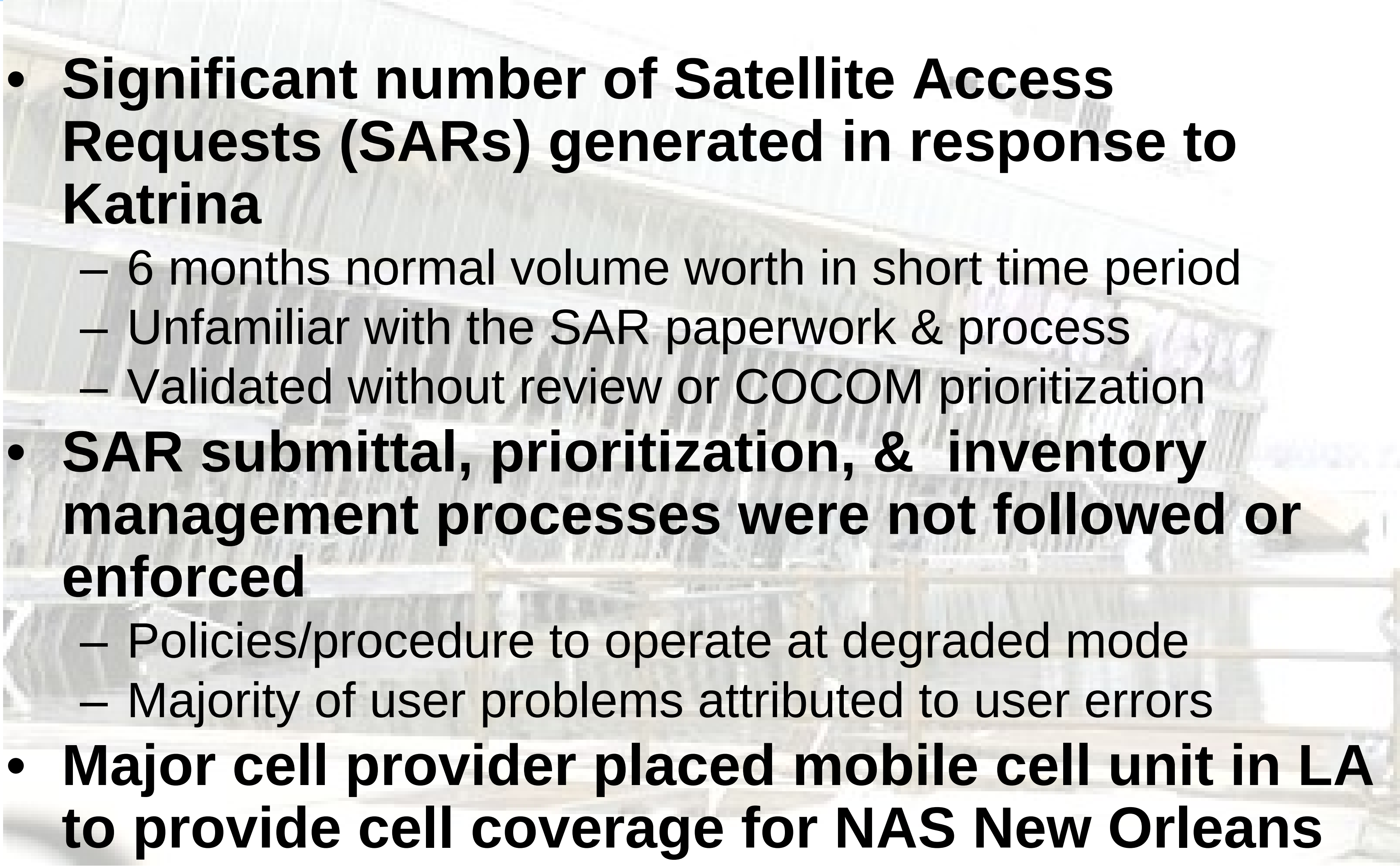
- ***Timely, Reliable Access to Data and Information Services for Authorized Users***

Katrina Events/SITREPs (Alternate Paths)



- **Increased need for DoD & Non- DoD SATCOM when ground based infrastructure is not available**
  - Satellite, handheld assets (Iridium, Blackberry), microwave networks
  - Numerous Satellite trucks/phones
  - Cellular on Wheels (COW) and Satellite Cellular on Light Truck (COLT)
- **Transportable 911 call center deployed to assist in restoring 911 services**
- **Government Emergency Telecommunications Service (GETS) performed well**

Katrina Events/SITREPs (Alternate Paths)



- **Significant number of Satellite Access Requests (SARs) generated in response to Katrina**
  - – 6 months normal volume worth in short time period
  - – Unfamiliar with the SAR paperwork & process
  - – Validated without review or COCOM prioritization
- **SAR submittal, prioritization, & inventory management processes were not followed or enforced**
  - – Policies/procedure to operate at degraded mode
  - – Majority of user problems attributed to user errors
- **Major cell provider placed mobile cell unit in LA to provide cell coverage for NAS New Orleans**

Katrina Events/SITREPs (Content Staging & Access)

- **Critical time-sensitive data required by non-DoD**
  - Content Staging allows accumulation of multi-source data to happen
  - State/Local Governments and First Responders require access support recovery/relief efforts in affected regions
- **Homeland Security cannot be carried out effectively on military networks to which non-DoD users don’t have access**
  - Need appropriate access control policy and mechanisms
- **Aggregation of data may result in an increase in classification**

Lesson Learned from NTCS New Orleans

- **Never build an IT facility on a coastline**
- **Never build on the first floor in a flood-prone area**
- **Make certain electricians remain on base to baby-sit the generators**
- **Never include windows on a computer floor**
- **Establish a yearly Preventative Maintenance contract to test UPS batteries at least once a year for under-load voltage <u>and</u> internal resistance**

Lesson Learned from NTCS New Orleans

- Make certain that all critical personnel have cell phones
- Make certain that all critical personnel have a hardcopy of important contacts
- Make certain that all critical personnel take a hardcopy of important contacts with them when/if they have to evacuate
- Put major systems on support/maintenance contracts with the manufacturer, include emergency response service

Summary

- **COOP Plans in-place and successfully executed**
  - Real-life experience in previous natural disasters helped w/training and planning
  - Many IA lessons learned from Katrina not applicable to 9/11
- **Certain applications were severely impacted after Katrina**
  - Fail-over to alternate paths increases latency
    - **Rerouted paths may provide connectivity, but may not provide sufficient Quality of Service for key applications**
    - **Policies/procedures to operate in degraded mode**
- **GIG can support Homeland Defense by providing critical data to non-DoD users**
  - Develop policies and procedures to allow access to assemble and disseminate critical data

Recommendations

- **Review COOP Plans to incorporate Katrina Lessons Learned**
- **Establish a portal front-end that supports the staging and discovery of unclassified information**
- **Ensure personnel are trained to handle increased SATCOM requirements during a crisis**
  - Include higher echelon review and prioritization responsibilities
  - Identify an office responsible for interfacing with commercial SATCOM providers
- **Develop specific policy to clarify roles, responsibilities and procedures when non-DoD users connect to the GIG**